

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANDERSON GARCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE TELECOMUNICACIONES

CALI

2020

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANDERSON GARCIA

Diplomado de opción de grado presentado para optar el  
título de INGENIERO DE TELECOMUNICACIONES

Director /Tutor

Efraín Alejandro Pérez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE TELECOMUNICACIONES

CALI

2020

NOTA DE ACEPTACIÓN:

---

---

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

Cali, (mayo 15, 2020)

## **AGRADECIMIENTOS**

A Dios quien ha sido mi guía, fortaleza y su mano de fidelidad y amor han estado conmigo hasta el día de hoy.

A mis padres quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.

## CONTENIDO

|  |    |
|--|----|
| LISTA DE TABLAS .....                                  | 6  |
| LISTA DE FIGURAS .....                                 | 7  |
| GLOSARIO.....  | 8  |
| RESUMEN.....   | 10 |
| ABSTRACT .....   | 10 |
| INTRODUCCION.....                                      | 11 |
| DESARROLLO DE LOS ESCENARIOS .....                     | 12 |
| Escenario 1 .....                                      | 12 |
| Relación de vecino BGP entre R1 y R2 .....             | 13 |
| Relación de vecino BGP entre R2 y R3 .....             | 15 |
| Relación de vecino BGP entre R3 y R4 .....             | 17 |
| Escenario 2 .....                                      | 19 |
| A. Configurar VTP.....                                 | 19 |
| B. Configurar DTP (Dynamic Trunking Protocol).....     | 22 |
| C. Agregar VLANs y asignar puertos.....                | 24 |
| D. Configurar las direcciones IP en los Switches. .... | 28 |
| E. Verificar la conectividad Extremo a Extremo .....   | 29 |
| CONCLUSIONES .....                                     | 35 |
| BIBLIOGRAFIA.....                                      | 36 |

## LISTA DE TABLAS

|  |    |
|--|----|
| Tabla 1. interfaz, dirección IP y máscara. ....        | 12 |
| Tabla 2. Tabla de direcciones para PCS. ....           | 27 |
| Tabla 3. Tabla de direccionamiento de PC. ....         | 28 |
| Tabla 4. Tabla de direccionamiento de los switch. .... | 28 |

## LISTA DE FIGURAS

|   |    |
|---|----|
| Figura 1. Escenario 2.....                  | 12 |
| Figura 2. Rutas vecinas entre R1 y R2. .... | 14 |
| Figura 3. Rutas vecinas entre R1 y R2. .... | 14 |
| Figura 4. Rutas vecinas entre R2 y R3. .... | 16 |
| Figura 5. Rutas vecinas entre R2 y R3. .... | 16 |
| Figura 6. Rutas vecinas entre R3 y R4. .... | 18 |
| Figura 7. Rutas vecinas entre R3 y R4. .... | 18 |
| Figura 8. Escenario 3.....                  | 19 |
| Figura 9. Status del SW en VTP. ....        | 20 |
| Figura 10. Status del SW en VTP. ....       | 21 |
| Figura 11. Status del SW en VTP. ....       | 21 |
| Figura 12. Modo trunk de los puertos. ....  | 22 |
| Figura 13. Modo trunk de los puertos. ....  | 23 |
| Figura 14. Modo trunk de los puertos. ....  | 23 |
| Figura 15. Modo trunk de los puertos. ....  | 24 |
| Figura 16. Error en creación de VLAN. ....  | 24 |
| Figura 17. VLAN creadas en el SW. ....      | 25 |
| Figura 18. VLAN creadas por VTP en SW.....  | 26 |
| Figura 19. VLAN creadas por VTP en SW.....  | 26 |
| Figura 20. Prueba de conectividad. ....     | 29 |
| Figura 21. Prueba de conectividad. ....     | 30 |
| Figura 22. Prueba de conectividad. ....     | 30 |
| Figura 23. Prueba de conectividad. ....     | 31 |
| Figura 24. Prueba de Conectividad.....      | 32 |
| Figura 25. Prueba de conectividad. ....     | 33 |
| Figura 26. Prueba de conectividad. ....     | 33 |
| Figura 27. Prueba de conectividad. ....     | 34 |

## **GLOSARIO**

**CCNP:** son las siglas de Cisco Certified Networking Professional. Es decir, un certificado de networking y telecomunicaciones. Lo que ofrece y avala es un dominio mayor sobre el sector y sus conocimientos, así como la materia.

**CISCO:** Cisco Systems es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones. Cisco Systems tiene productos para routing (redes), seguridad, colaboración (telefonía IP y sistemas de videoconferencia), data center, cloud y movilidad (wireless).

**Red LAN:** es una sigla que refiere a Local Area Network (Red de Área Local). Estas redes vinculan computadoras que se hallan en un espacio físico pequeño, como una oficina o un edificio. La interconexión se realiza a través de un cable o de ondas.

**Router:** enrutador (del inglés router) o encaminador es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.



Switch: un switch o conmutador es un dispositivo de interconexión de redes informáticas. En computación y en informática de redes, un switch es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI u Open Systems Interconnection.

VLAN: es un acrónimo que deriva de una expresión inglesa: virtual LAN. Esa expresión, por su parte, alude a una sigla ya que LAN significa Local Area Network. De este modo, podemos afirmar que la idea de VLAN refiere a una red de área local (lo que conocemos como LAN) de carácter virtual.

## **RESUMEN**

La configuración de protocolos de enrutamiento de paquetes en dispositivos de capa 2 y 3, son indispensables para el buen funcionamiento de una red, cisco a través de su academia ccnp, brinda los conocimientos necesarios para lograr los escenarios que se desarrollaran en este trabajo, como la configuración de BGP, para establecer la conexión entre vecinos de diferentes ids y VTP, para que los dispositivos de capa dos se comporten como replicadores del switch modo server. Desarrollado en simuladores propios de cisco.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

## **ABSTRACT**

The configuration of packet routing protocols in layer 2 and 3 devices are essential for the proper functioning of a network, cisco through its ccnp academy, provides the necessary knowledge to achieve the scenarios that will be developed in this work, such as the BGP configuration, to establish the connection between neighbors of different ids and VTP, so that the layer two devices behave like replicators of the server mode switch. Developed in cisco's own simulators.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

## INTRODUCCION

Con el Diplomado CCNP se consiguen las competencias para configurar, administrar y resolver fallas en redes empresariales medianas y grandes de tipo LAN y WAN, involucrando tecnologías convergentes en seguridad, datos. Estos conocimientos están dirigidos a ingenieros, tecnólogos y técnicos con al menos un año de experiencia en administración de redes, que desean mejorar sus habilidades y/o trabajar de forma independiente en soluciones de redes complejas.

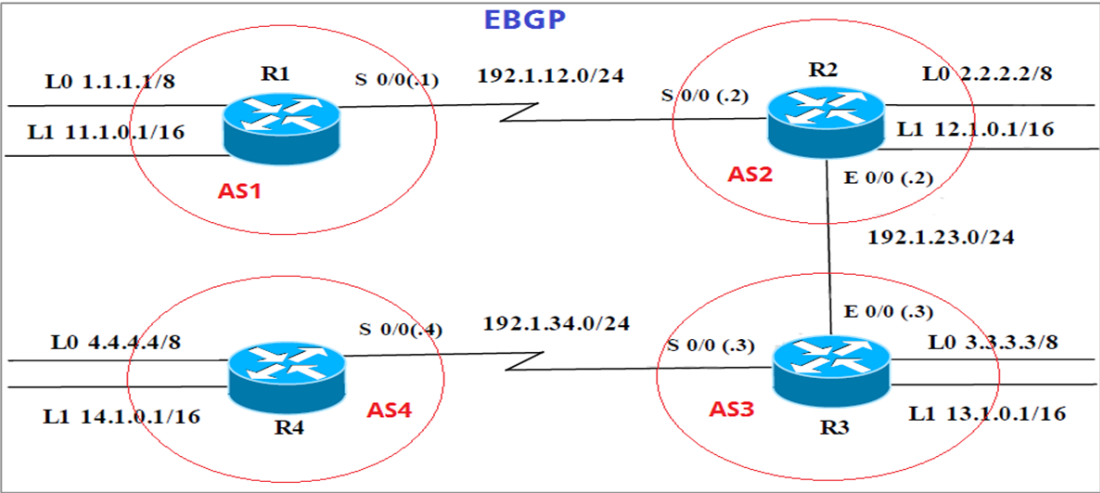
BGP como protocolo de enrutamiento presenta un grado de dificultad mayor que los protocolos vector distancia, ya que sus configuración son un poco más extensa y laboriosas a la hora de realizar una implementación como la presenta el ejercicio desarrollado, el simulador GNS, brinda las herramientas necesarias para lograr laboratorios con complejidades mayores a los permitidos en packet tracer

El protocolo vtp brinda una sencillez impresionante a la hora de lograr compartir la información de vlan, en los dispositivos configurados para este fin. La facilidad que presta el simulador de la academia en replicar la configuración, a través de la herramienta de telnet, facilita el trabajo y reduce los tiempos, y gracias a su ayuda se puede reproducir en dispositivos reales.

# DESARROLLO DE LOS ESCENARIOS

## Escenario 1

Figura 1. Escenario 2.



Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

Tabla 1. interfaz, dirección IP y máscara.

R1

| Interfaz   | Dirección IP | Máscara       |
|------------|--------------|---------------|
| Loopback 0 | 1.1.1.1      | 255.0.0.0     |
| Loopback 1 | 11.1.0.1     | 255.255.0.0   |
| S 0/0      | 192.1.12.1   | 255.255.255.0 |

R2

| Interfaz   | Dirección IP | Máscara       |
|------------|--------------|---------------|
| Loopback 0 | 2.2.2.2      | 255.0.0.0     |
| Loopback 1 | 12.1.0.1     | 255.255.0.0   |
| S 0/0      | 192.1.12.2   | 255.255.255.0 |
| E 0/0      | 192.1.23.2   | 255.255.255.0 |

R3

| Interfaz   | Dirección IP | Máscara       |
|------------|--------------|---------------|
| Loopback 0 | 3.3.3.3      | 255.0.0.0     |
| Loopback 1 | 13.1.0.1     | 255.255.0.0   |
| E 0/0      | 192.1.23.3   | 255.255.255.0 |
| S 0/0      | 192.1.34.3   | 255.255.255.0 |

R4

| Interfaz   | Dirección IP | Máscara       |
|------------|--------------|---------------|
| Loopback 0 | 4.4.4.4      | 255.0.0.0     |
| Loopback 1 | 14.1.0.1     | 255.255.0.0   |
| S 0/0      | 192.1.34.3   | 255.255.255.0 |

Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

## Relación de vecino BGP entre R1 y R2

Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
R1(config)#hostname R1
R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#interface serial 0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#exit
R1(config)#do wr
Building configuration...
```

```
R2(config)#hostname R2
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface Loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#interface serial 0/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface e1/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
```

Figura 2. Rutas vecinas entre R1 y R2.

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
C    1.0.0.0/8 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:01:44
     11.0.0.0/16 is subnetted, 1 subnets
C      11.1.0.0 is directly connected, Loopback1
     12.0.0.0/16 is subnetted, 1 subnets
B      12.1.0.0 [20/0] via 192.1.12.2, 00:01:44
R1#
```

Fuente: Elaboración propia.

Figura 3. Rutas vecinas entre R1 y R2.

```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:02:53
C    2.0.0.0/8 is directly connected, Loopback0
C    192.1.23.0/24 is directly connected, Ethernet1/0
     11.0.0.0/16 is subnetted, 1 subnets
B      11.1.0.0 [20/0] via 192.1.12.1, 00:02:53
     12.0.0.0/16 is subnetted, 1 subnets
C      12.1.0.0 is directly connected, Loopback1
R2#
```

Fuente: Elaboración propia.

## Relación de vecino BGP entre R2 y R3

Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
R2(config)#router bgp 2
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#do wr
Building configuration...
```

```
R3(config)#hostname R3
R3(config)#interface Loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface e1/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 0/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

Figura 4. Rutas vecinas entre R2 y R3.

```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:06:17
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:23
C    192.1.23.0/24 is directly connected, Ethernet1/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:06:17
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.23.3, 00:00:25
R2#
```

Fuente: Elaboración propia.

Figura 5. Rutas vecinas entre R2 y R3.

```
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:01:06
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:01:06
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:01:06
C    3.0.0.0/8 is directly connected, Loopback0
C    192.1.23.0/24 is directly connected, Ethernet1/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:01:06
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:01:06
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
R3#
```

Fuente: Elaboración propia.



### Relación de vecino BGP entre R3 y R4

Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
R3(config)#router bgp 3
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
R3(config-router)#no neighbor 192.1.34.4
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0
R3(config-router)#neighbor 4.4.4.4 remote-as 4
R3(config-router)#neighbor 4.4.4.4 update-source loopback 0
R3(config-router)# neighbor 4.4.4.4 ebgp-multihop
```

```
R4(config)#hostname R4
R4(config)#interface Loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface serial 0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#exit
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)#neighbor 3.3.3.3 remote-as 4
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)# neighbor 3.3.3.3 ebgp-multihop
R4(config-router)#do wr
Building configuration...
```

Figura 6. Rutas vecinas entre R3 y R4.

```
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:05:51
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:05:51
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:05:51
C    3.0.0.0/8 is directly connected, Loopback0
S    4.0.0.0/8 [1/0] via 192.1.34.4
C    192.1.23.0/24 is directly connected, Ethernet1/0
     11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.23.2, 00:05:51
C    192.1.34.0/24 is directly connected, Serial0/0
     12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:05:52
     13.0.0.0/16 is subnetted, 1 subnets
C        13.1.0.0 is directly connected, Loopback1
R3#
```

Fuente: Elaboración propia.

Figura 7. Rutas vecinas entre R3 y R4.

```
R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

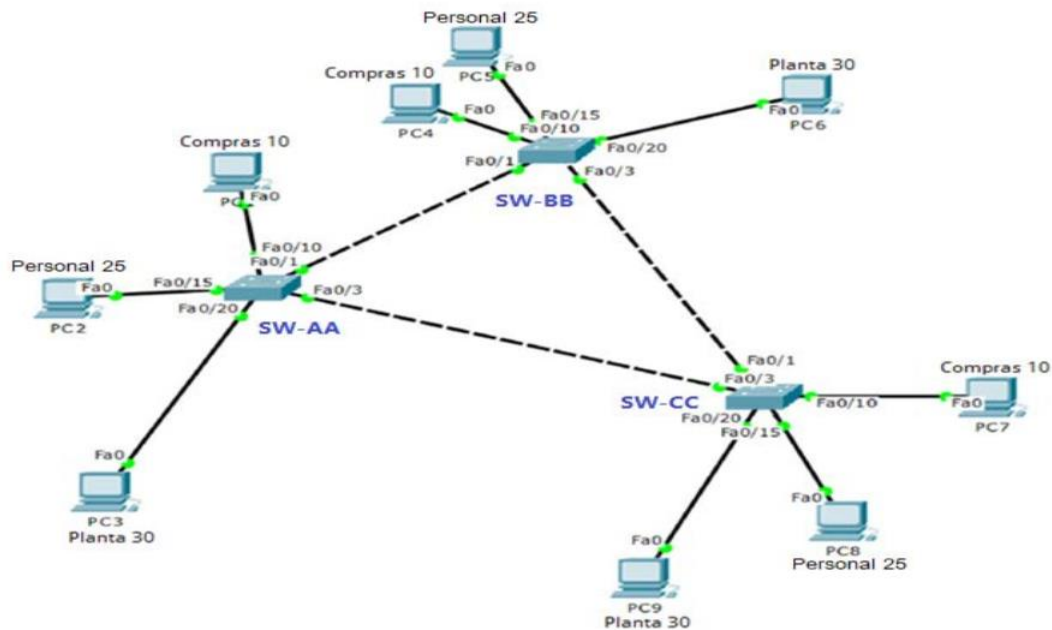
Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 3.3.3.3, 00:46:50
B    1.0.0.0/8 [20/0] via 3.3.3.3, 00:46:50
B    2.0.0.0/8 [20/0] via 3.3.3.3, 00:46:50
S    3.0.0.0/8 [1/0] via 192.1.34.3
C    4.0.0.0/8 is directly connected, Loopback0
B    192.1.23.0/24 [20/0] via 3.3.3.3, 00:46:50
     11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 3.3.3.3, 00:46:50
C    192.1.34.0/24 is directly connected, Serial1/0
     12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 3.3.3.3, 00:46:50
     13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 3.3.3.3, 00:46:50
     14.0.0.0/16 is subnetted, 1 subnets
C        14.1.0.0 is directly connected, Loopback1
R4#
```

Fuente: Elaboración propia.

## Escenario 2

Figura 8. Escenario 3.



Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

### A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN.

El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VTP llamado CCNP y usando la contraseña cisco.

#### Switch 1

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-AA
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Domain name already set to CCNP.
SW-AA(config)#vtp password cisco
Password already set to cisco
```

Switch 2

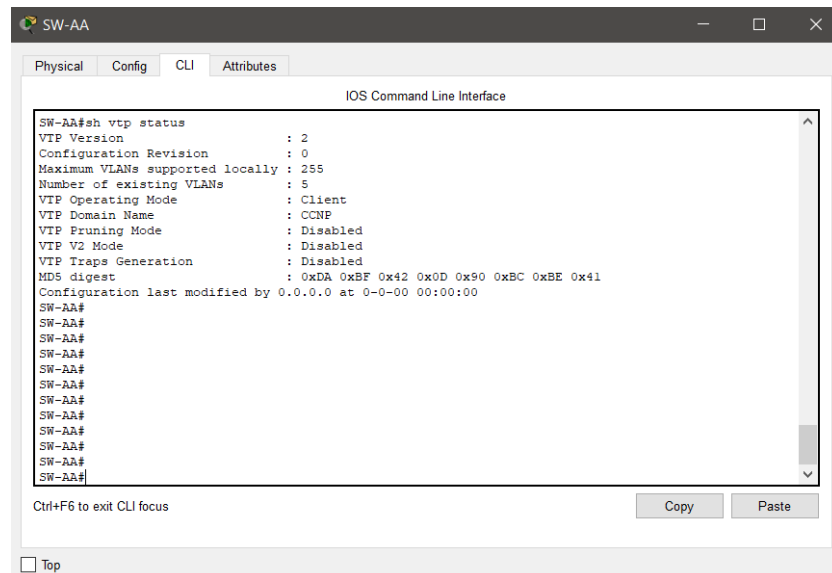
```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco
```

Switch 3

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
```

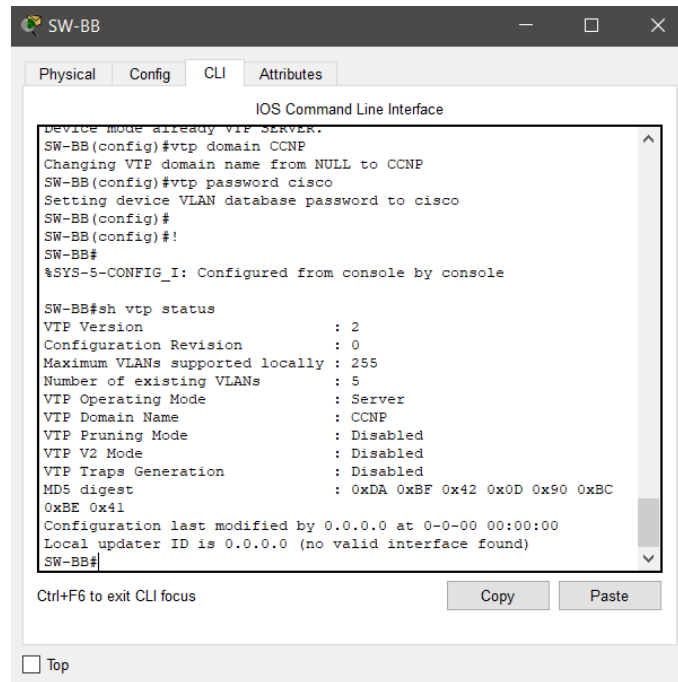
2. Verifique las configuraciones mediante el comando show vtp status.

*Figura 9. Status del SW en VTP.*



*Fuente: Elaboración propia.*

Figura 10. Status del SW en VTP.



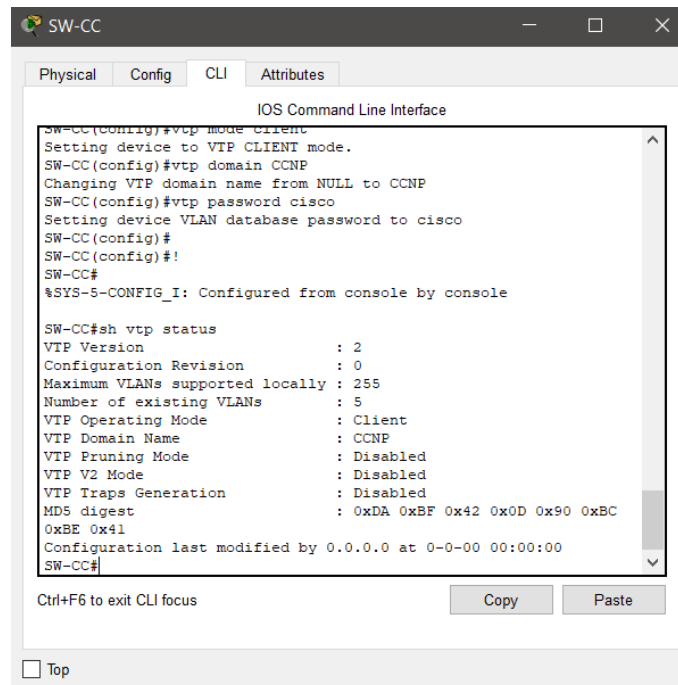
The screenshot shows the CLI of a switch named SW-BB. The user has entered the command `sh vtp status`, which displays the following configuration details:

```
SW-BB#sh vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             : CCNP
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xDA 0xBF 0x42 0x0D 0x90 0xBC
0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
```

Below the output, there are buttons for 'Copy' and 'Paste', and a 'Top' link.

Fuente: Elaboración propia.

Figura 11. Status del SW en VTP.



The screenshot shows the CLI of a switch named SW-CC. The user has entered the command `sh vtp status`, which displays the following configuration details:

```
SW-CC#sh vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Client
VTP Domain Name             : CCNP
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xDA 0xBF 0x42 0x0D 0x90 0xBC
0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-CC#
```

Below the output, there are buttons for 'Copy' and 'Paste', and a 'Top' link.

Fuente: Elaboración propia.

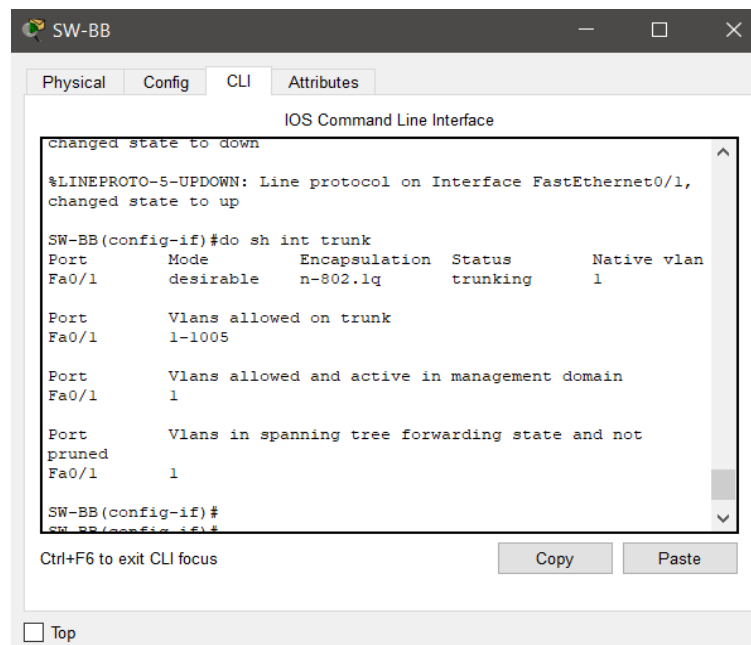
## B. Configurar DTP (Dynamic Trunking Protocol)

1. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

```
SW-BB(config)#interface fastEthernet 0/1
SW-BB(config-if)#switchport mode dynamic desirable
```

2. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando **show interfaces trunk**.

Figura 12. Modo trunk de los puertos.



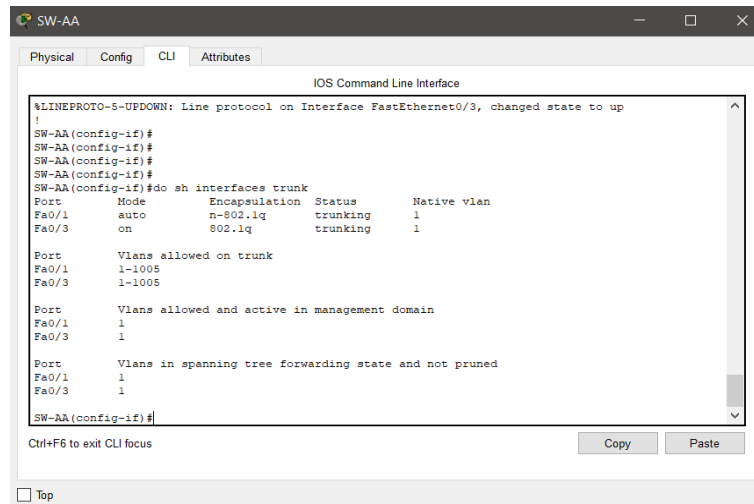
Fuente: Elaboración propia.

3. Entre SW-AA y SW-CC configure un enlace "trunk" estático utilizando el comando **switchport mode trunk** en la interfaz F0/3 de SW-AA.

```
SW-AA(config)#interface fastEthernet 0/3
SW-AA(config-if)#switchport mode trunk
```

4. Verifique el enlace "trunk" el comando **show interfaces trunk** en SW-AA.

Figura 13. Modo trunk de los puertos.



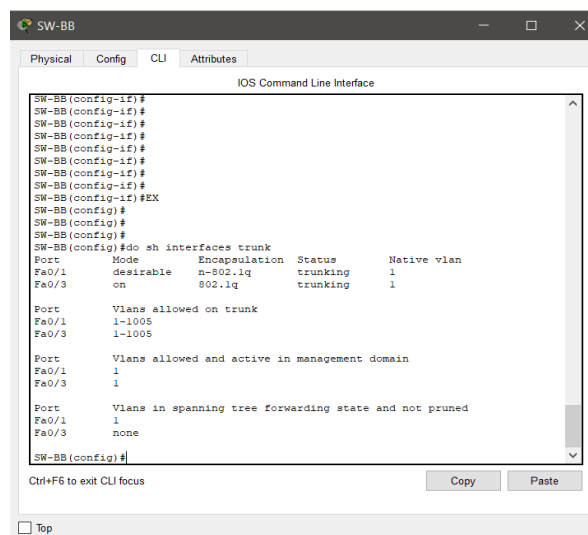
Fuente: Elaboración propia.

5. Configure un enlace "trunk" permanente entre SW-BB y SW-CC.

```
SW-CC(config)#interface fastEthernet 0/1  
SW-CC(config-if)#switchport mode trunk
```

```
SW-BB(config)#interface fastEthernet 0/3  
SW-BB(config-if)#switchport mode trunk
```

Figura 14. Modo trunk de los puertos.



Fuente: Elaboración propia.

Figura 15. Modo trunk de los puertos.

```

SW-CC(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to up
SW-CC(config-if)#ex
SW-CC(config)#
SW-CC(config)#
SW-CC(config)#
SW-CC(config)#
SW-CC(config)#do sh interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q          trunking    1
Fa0/3     auto      n-802.1q        trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     1
SW-CC(config)#
  
```

Fuente: Elaboración propia.

## C. Agregar VLANs y asignar puertos.

1. En STW1 agregue la VLAN 10. En STW2 agregue las VLANs Compras (10), Personal (20), Planta (30) y Admon (99).

SW-AA(config)#vlan 10

Figura 16. Error en creación de VLAN.

```

SW-AA>
SW-AA>
SW-AA>
SW-AA>en
SW-AA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#
SW-AA(config)#
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config)#
  
```

Fuente: Elaboración propia.



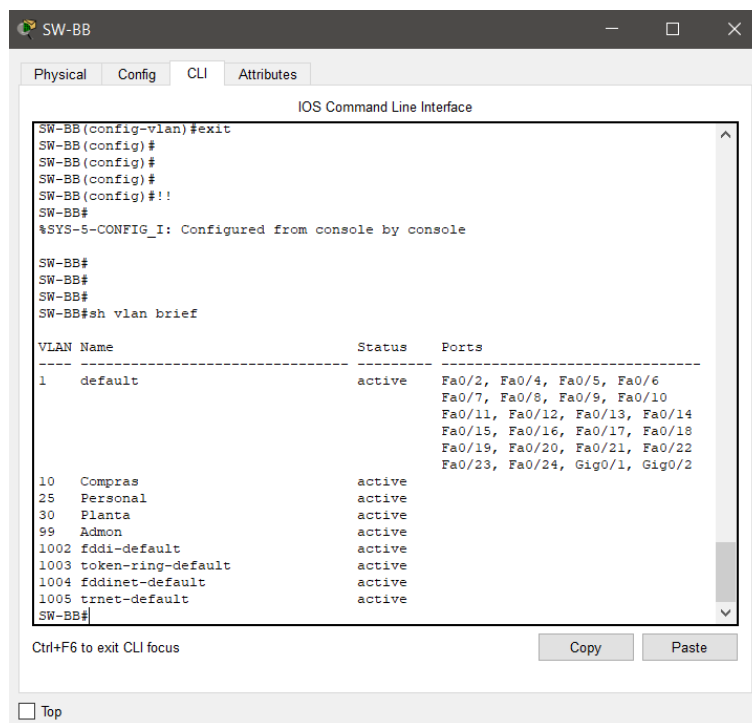
```

SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit

```

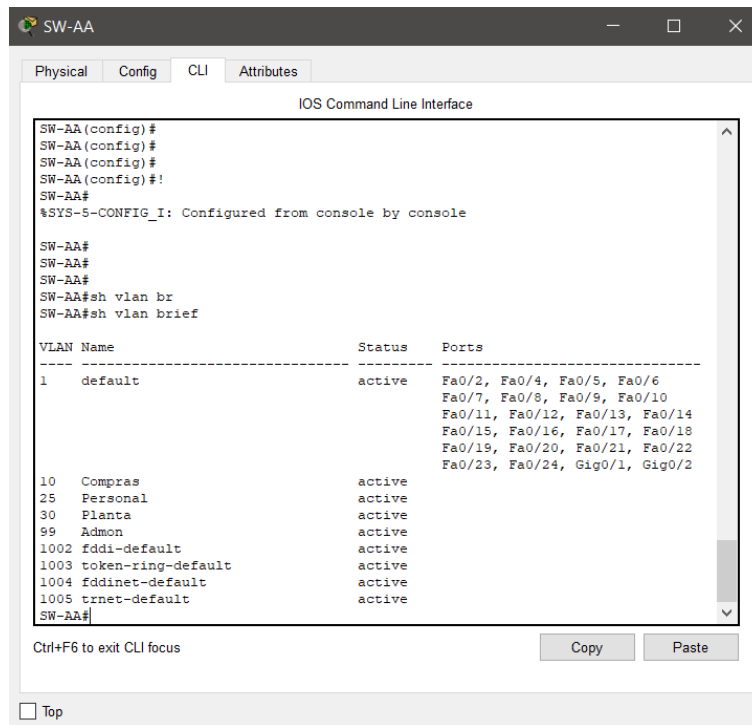
## 2. Verifique que las VLANs han sido agregadas correctamente.

Figura 17. VLAN creadas en el SW.



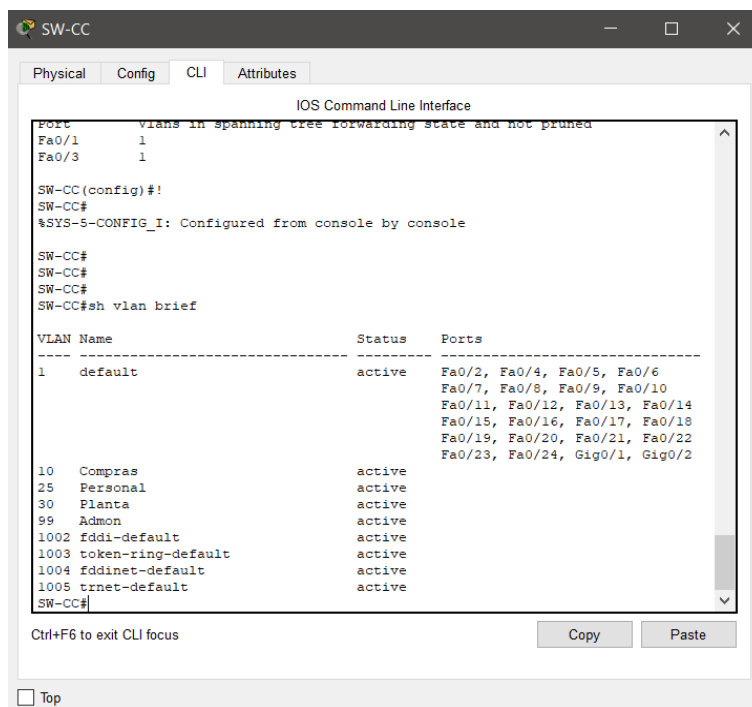
Fuente: Elaboración propia.

Figura 18. VLAN creadas por VTP en SW.



Fuente: Elaboración propia.

Figura 19. VLAN creadas por VTP en SW.



Fuente: Elaboración propia.

3. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

*Tabla 2. Tabla de direcciones para PCs.*

| Interfaz | VLAN    | Direcciones IP de los PCs |
|----------|---------|---------------------------|
| F0/10    | VLAN 10 | 190.108.10.X /24          |
| F0/15    | VLAN 25 | 190.108.20.X /24          |
| F0/20    | VLAN 30 | 190.108.30.X /24          |

X = número de cada PC particular

*Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.*

4. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.
5. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC.

Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

```
SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
```

```
SW-BB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode access
```

```

SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30

```

```

SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30

```

Tabla 3. Tabla de direccionamiento de PC.

| Pc | Vlan | Ip           | Mascara       |
|----|------|--------------|---------------|
| 1  | 10   | 190.108.10.1 | 255.255.255.0 |
| 4  | 10   | 190.108.10.2 | 255.255.255.0 |
| 7  | 10   | 190.108.10.3 | 255.255.255.0 |
| 2  | 20   | 190.108.20.4 | 255.255.255.0 |
| 5  | 20   | 190.108.20.5 | 255.255.255.0 |
| 8  | 20   | 190.108.20.6 | 255.255.255.0 |
| 3  | 30   | 190.108.30.7 | 255.255.255.0 |
| 6  | 30   | 190.108.30.8 | 255.255.255.0 |
| 9  | 30   | 190.108.30.9 | 255.255.255.0 |

Fuente: Elaboración propia.

## D. Configurar las direcciones IP en los Switches.

1. En cada uno de los Switches asigne una dirección IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Tabla 4. Tabla de direccionamiento de los switch.

| Equipo | Interfaz | Dirección IP | Máscara      |
|--------|----------|--------------|--------------|
| SW-AA  | VLAN 99  | 190.108.99.1 | 255.255.255. |
| SW-BB  | VLAN 99  | 190.108.99.2 | 255.255.255. |
| SW-CC  | VLAN 99  | 190.108.99.3 | 255.255.255. |

Fuente: Elaboración propia.

```
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
```

```
SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
```

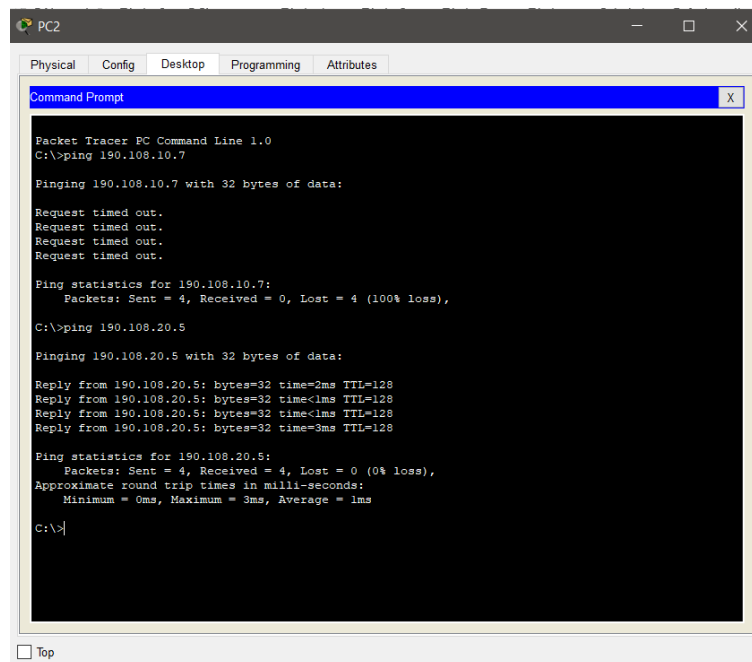
```
W-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
```

## E. Verificar la conectividad Extremo a Extremo

1. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

### Ping de PC2 a PC4 y PC8

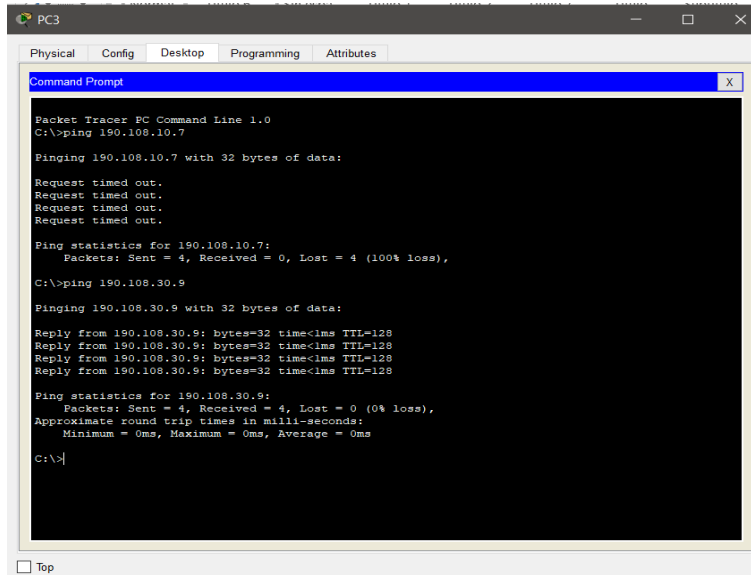
*Figura 20. Prueba de conectividad.*



*Fuente: Elaboración propia.*

## Ping de PC3 a PC5 y PC6

Figura 21. Prueba de conectividad.



```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.7

Pinging 190.108.10.7 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.9

Pinging 190.108.30.9 with 32 bytes of data:

Reply from 190.108.30.9: bytes=32 time<1ms TTL=128
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128

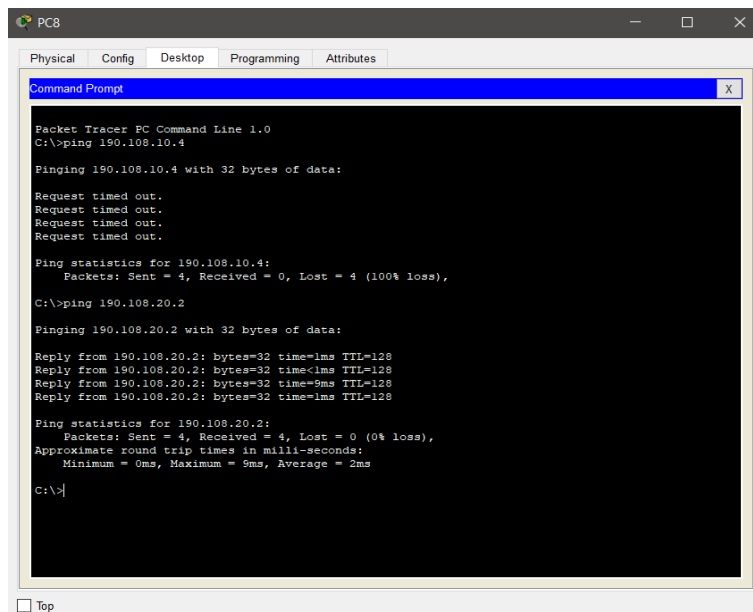
Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Elaboración propia.

## Ping de PC1 a PC3 y PC2

Figura 22. Prueba de conectividad.



```
PC8
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.4

Pinging 190.108.10.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.2

Pinging 190.108.20.2 with 32 bytes of data:

Reply from 190.108.20.2: bytes=32 time<1ms TTL=128
Reply from 190.108.20.2: bytes=32 time<1ms TTL=128
Reply from 190.108.20.2: bytes=32 time=9ms TTL=128
Reply from 190.108.20.2: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>
```

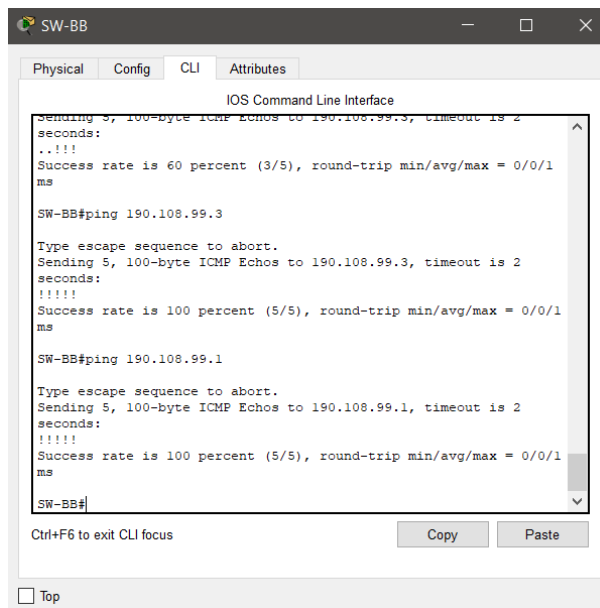
Fuente: Elaboración propia.

Vtp es un protocolo que se encarga de compartir la información de vlan entre sw, mas no permite que la comunicación de paquetes entre redes diferentes, ese es el motivo por el cual no se comunican esos pcs pero si funcionan entre los que se encuentra conectados en la misma vlan

2. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.

## Ping de SW-BB a SW-AA Y SW-CC

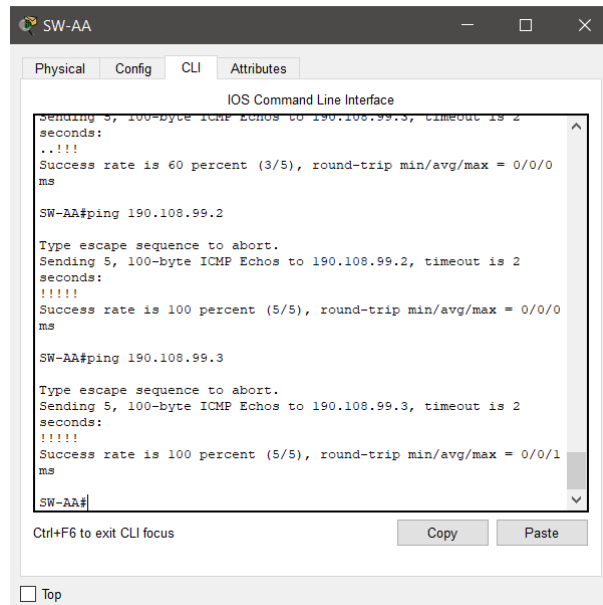
Figura 23. Prueba de conectividad.



Fuente: Elaboración propia.

## Ping de SW-AA a SW-BB Y SW-CC

Figura 24. Prueba de Conectividad.



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2
seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0
ms
SW-AA#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0
ms
SW-AA#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1
ms
SW-AA#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

Fuente: Elaboración propia.

La comunicación entre sw es exitosa ya que ellos comparten direcciones entre la misma red y la comunicación entre ellos es tan sencilla como comunicar dos pcs por un cable cruzado

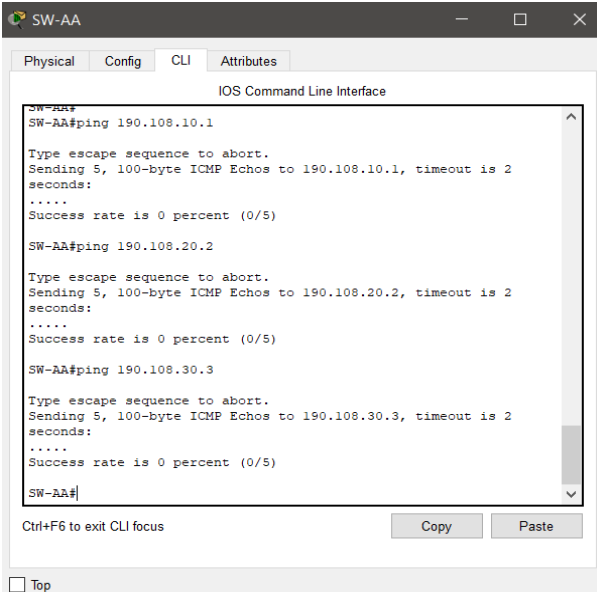
3. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito.

El ping realizado entre los Switches y los PCs no tuvo éxito. Ya que, si bien se tienen habilitadas las VLANs en cada uno de los Switches a través del protocolo VTP, y se configuro cada una de las interfaces que conectan los switches a los PCs en modo de acceso según la respectiva VLAN a la cual pertenecen, aun no se configura un enrutamiento IP en las VLANs creadas.



## Ping de SW-AA a PC1-PC2 y PC3

Figura 25. Prueba de conectividad.



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA#ping 190.108.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.2, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#
```

Ctrl+F6 to exit CLI focus

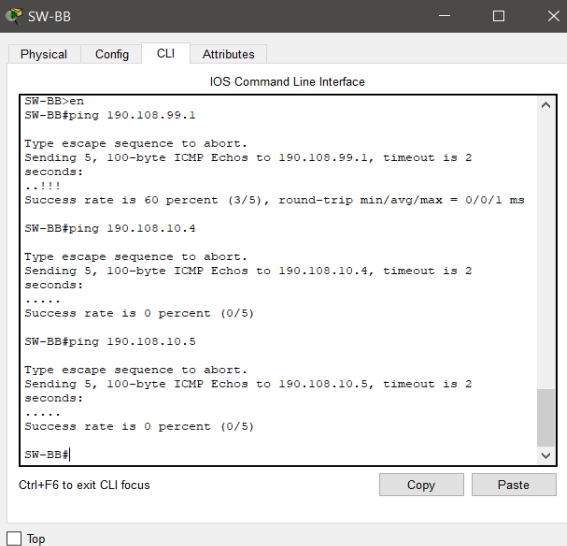
Copy Paste

☐ Top

Fuente: Elaboración propia.

## Ping de SW-BB a PC4-PC5 y PC6

Figura 26. Prueba de conectividad.



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
SW-BB>en
SW-BB#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2
seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/1 ms

SW-BB#ping 190.108.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.10.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.5, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#
```

Ctrl+F6 to exit CLI focus

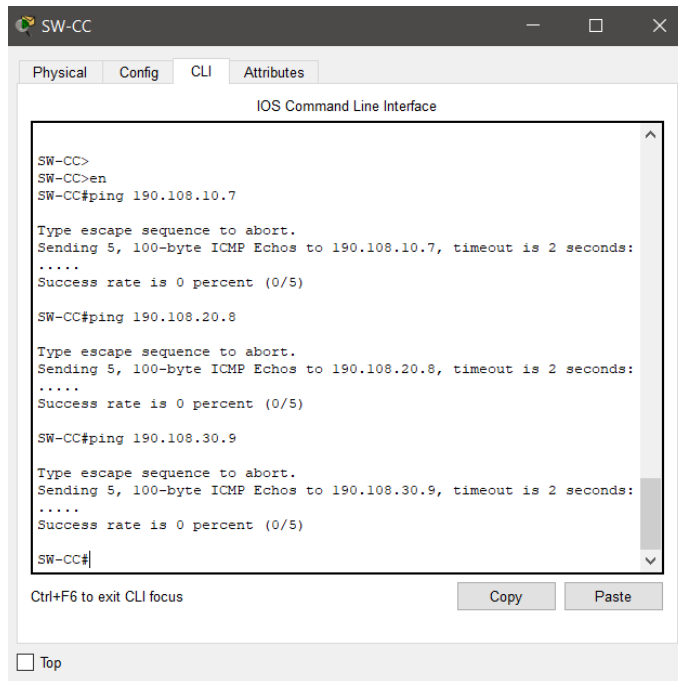
Copy Paste

☐ Top

Fuente: Elaboración propia.

## Ping de SW-CC a PC7-PC8 y PC9

Figura 27. Prueba de conectividad.



Fuente: Elaboración propia.

## CONCLUSIONES

El diplomado en CCNP ofrece conocimientos avanzados sobre redes que permiten instalar, configurar y manejar redes LAN, WAN y servicios de acceso para organizaciones que necesiten implementaciones avanzadas a para sus procesos

Aunque BGP puede llegar a ser complejo, presta una facilidad en el enrutamiento de paquetes de nivel WAN ya que su estructura permite que los paquetes viajen con mayor facilidad entre los router, no es aconsejable su implementación en redes de área local ni entornos corporativos.

VTP es un protocolo que en redes LAN, funciona de maravilla pero siempre se debe complementar con el protocolo Spanning Tree, ya que VTP no trabaja sobre las colisiones de paquetes en dominio de broadcast por lo que la ruta para que las vlan se comuniquen siempre va a ser el mismo y va a causar, flujo de información de mas en los cables que comunican los switch

## BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Architecture.

Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado

de: <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de <https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppI>